CLAIMS

What is claimed is:

1. A method of deterring a rollback attack against a first database comprising:

determining if the first database is corrupted, the first database being associated with a first authentication code;

determining if a second database is corrupted when the first database is corrupted, the second database being associated with a second authentication code, the second database having contents substantially the same as the first database;

when the second database is not corrupted, recalculating the second authentication code using a portion of the first authentication code, copying the second database over the first database, and proceeding with authorized operations for processing content by an application program.

2. The method of claim 1, when the second database is not corrupted, further comprising presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining validity of the passcode, and performing the recalculating and copying only when the passcode is valid.

3. The method of claim 1, further comprising continuing with authorized operations of the application program for processing content when the first database is not corrupted.

4. The method of claim 1, wherein the first database comprises usage rules for processing selected content by the application program, the usage rules including a copy count for the selected content.

5. The method of claim 1, wherein the content comprises digital audio data.

6. The method of claim 5, wherein the application program complies with requirements for a secure digital music initiative (SDMI) implementation.

7. The method of claim 1, wherein the first authentication code comprises a hash of the first database and a first secret, and the second authentication code comprises a hash of the second database and a second secret, the first secret being different than the second secret.

8. The method of claim 7, wherein the portion comprises the first secret.

9. The method of claim 2, further comprising allowing a predetermined number of operations of copying the second database over the first database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode.

10. An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for deterring a rollback attack against a first database by determining if the first database is corrupted, the first database being associated with a first authentication code, by determining if a second database is corrupted when the first database is corrupted, the second database being associated with a second authentication code, the second database having contents substantially the same as the first database, and when the second database is not corrupted, recalculating the second authentication code using a portion of the first authentication code, copying the second database over the first database, and proceeding with authorized operations for processing content by an application program.

11. The article of claim 10, when the second database is not corrupted, further comprising instructions for presenting a challenge code to a user of the application program, for requiring the user to obtain a passcode in response to the challenge code, and for determining validity of the passcode, and for performing the recalculating and copying only when the passcode is valid.

12. The article of claim 10, further comprising instructions for continuing with authorized operations of the application program for processing content when the first database is not corrupted.

13. The article of claim 10, wherein the first database comprises usage rules for processing selected content by the application program, the usage rules including a copy count for the selected content.

14. The article of claim 10, wherein the content comprises digital audio data.

15. The article of claim 14, wherein the application program complies with requirements for a secure digital music initiative (SDMI) implementation.

16. The article of claim 10, wherein the first authentication code comprises a hash of the first database and a first secret, and the second authentication code comprises a hash of the second database and a second secret, the first secret being different than the second secret.

17. The article of claim 16, wherein the portion comprises the first secret.

18. The article of claim 11, further comprising instructions for allowing a predetermined number of operations of copying the second database over the first database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode.

19. A method of deterring circumvention of a content protection system of an application program via restoration of a first control database, the first control database being associated with the application program and including usage rules for digital audio content, comprising:

determining if the first control database is corrupted, the first control database being associated with a first message authentication code (MAC);

determining if a second control database is corrupted when the first control database is corrupted, the second control database being associated with a second message authentication code (MAC), the second control database having contents substantially the same as the first control database;

when the second control database is not corrupted, performing the following actions:

presenting a challenge code to a user of the application program;

requiring the user to obtain a passcode in response to the challenge code; and

determining validity of the passcode;

recalculating the second MAC using a portion of the first MAC and copying the second control database over the first control database when the passcode is valid; and

proceeding with authorized operations for processing the digital audio content by an application program consistent with the usage rules.

20. The method of claim 19, wherein the usage rules comprise a copy count for the digital audio content.

21. The method of claim 20, wherein the application program complies with requirements for a secure digital music initiative (SDMI) implementation.

22. The method of claim 19, wherein the first MAC comprises a hash of the first control database and a first secret, and the second MAC comprises a

hash of the second control database and a second secret, the first secret being different than the second secret.

23. The method of claim 19, further comprising allowing a predetermined number of operations of copying the second control database over the first control database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode.

24. The method of claim 19, wherein copying of the second control database over the first control database is performed after beginning execution of the application program but before proceeding with authorized operations for processing the digital audio content by an application program consistent with the usage rules.

25. An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for deterring circumvention of a content protection system of an application program via restoration of a first control database, the first control database being associated with the application program and including usage rules for digital audio content, by

determining if the first control database is corrupted, the first control database being associated with a first message authentication code (MAC);

determining if a second control database is corrupted when the first control database is corrupted, the second control database being associated with a second message authentication code (MAC), the second control database having contents substantially the same as the first control database;

when the second control database is not corrupted, performing the following actions:

presenting a challenge code to a user of the application program;

requiring the user to obtain a passcode in response to the challenge code; and

determining validity of the passcode;

recalculating the second MAC using a portion of the first MAC and copying the second control database over the first control database when the passcode is valid; and

proceeding with authorized operations for processing the digital audio content by an application program consistent with the usage rules.

26. The article of claim 25, wherein the usage rules comprise a copy count for the digital audio content.

27. The article of claim 25, wherein the first MAC comprises a hash of the first control database and a first secret, and the second MAC comprises a hash of the second control database and a second secret, the first secret being different than the second secret.

28. The article of claim 25, further comprising instructions for allowing a predetermined number of operations of copying the second control database over the first control database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode.